# Supplier Cyber Security Assessment Model Overview

## Introduction

Supply chain cyber security risk management continues to receive much industry and regulatory attention. The NATF and other industry organizations have worked together to produce guidance and tools to address various steps in the supply chain cyber security risk assessment lifecycle (Figure 1).[1]


**Figure 1: The Supply Chain Cyber Security Risk Assessment Lifecycle**

The NATF has created a supplier cyber security assessment model that:

1. Establishes criteria entities may use to evaluate supplier cyber security practices (NATF Criteria)
2. Suggests how entities obtain assurance of the supplier's adherence to the criteria

The NATF model and complementary products from other organizations provide tools for good cyber security practices that, executed properly, ensure compliance with the North American Electric Reliability Corporation's (NERC) supply chain reliability standards,[2] which become effective on July 1, 2020. Many of the criteria exceed what is required for compliance.

## Value Proposition

The NATF model and complementary products of other organizations provide a streamlined, effective, and efficient industry-accepted approach for entities to assess supplier cyber security practices, which, if applied widely, will reduce the burden on suppliers, provide entities with more and better information, and improve cyber security.

---

[1] In its August 2017 resolution adopting the supply chain standards, the NERC board of trustees requested NATF and other industry organizations to develop and share "best and leading practices in cyber security supply chain risk management, including procurement, specification, vendor requirements, and managing existing equipment activities." (*See* NERC Board of Trustees' Resolution)

[2] In response to FERC Order No. 829, NERC Reliability Standards Project 2016-03 Cyber Security Supply Chain Risk Management developed new Reliability Standard CIP-013-1 and modified Reliability Standards CIP-005-6 and CIP-010-3, which collectively have become known as the "supply chain standards."

## Description of the Model

The model uses the NATF Criteria to evaluate a supplier's cyber security practices. The criteria are mapped to the applicable requirements of the NERC standards and common industry security standards and frameworks and can be mapped to additional security standards or frameworks.

Adherence to the NATF Criteria can be demonstrated using existing industry security standards, frameworks, and assessment approaches, allowing suppliers to provide evidence from a certification or an independent assessment to show how the supplier's practices support each criterion.[3] When a third-party assessment is not available, suppliers may provide other evidence to demonstrate their adherence to the criterion (Figure 2).

Supplier responses are inputs into the entity's risk analysis for the supplier. Entities determine whether the information obtained from the supplier identifies risks in the supplier's cyber security practices, and whether these risks can be mitigated (by the entity or supplier) or accepted. This determination, along with other factors in the entity's risk analysis, will guide the entity's purchase decision.[4]

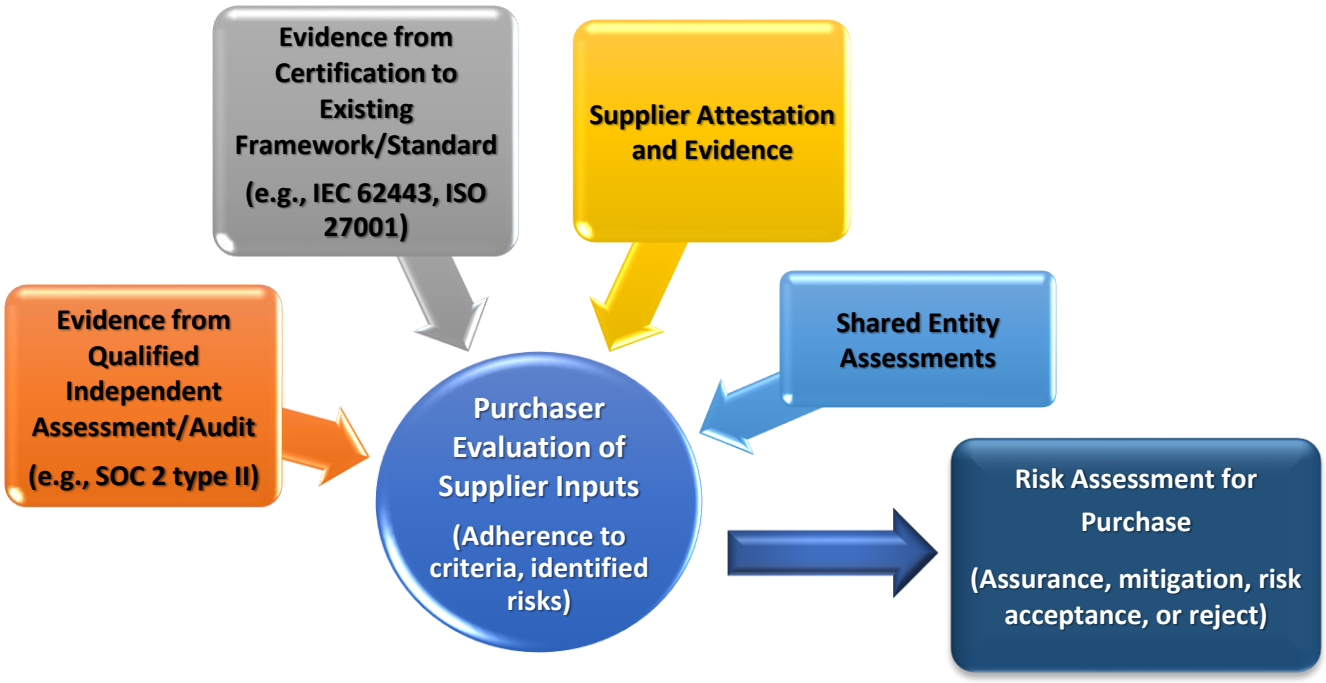


**Figure 2: Supplier Demonstration of Adherence to Criteria Supports Purchaser Risk Assessment**

[3] The use of an independent assessment to implement the cyber security supply chain risk management plan is described in the ERO Enterprise Endorsed Implementation Guidance "NATF CIP-013-1 Implementation Guidance."

[4] Whether an entity determines that the information obtained from a supplier identifies a risk may depend on many factors, including the risk of the product or service being purchased, the use of the product or service throughout the entity, the degree to which a supplier adheres to the criteria overall or to a specific criterion, and the level of assurance the supplier provides the entity of its adherence.

## Model Development and Relationship to Products of Other Organizations

The model was created by a diverse group of representatives from registered entities, major suppliers, and third-party assessors. Subsequently, the development team worked with other industry organizations to obtain input on the NATF Criteria, discuss and understand several on-going efforts to address supply chain cyber security, and to commit to making the products of these efforts work together. These complementary products and tools include, but are not limited to:

- Standardized questionnaires
- Standardized contract language
- Various databases providing basic information on how suppliers adhere to the criteria

In addition, suppliers and third-party assessors have expressed support for the model.

## Model Governance and Continuing Development

The model will mature as the industry recognizes the need to add criteria, revise existing criteria, and provide mapping to additional industry frameworks, but the goal of wide adoption requires that revisions be made in a predictable way with consensus from industry. The NATF, working with other industry organizations, will develop a governance policy to establish processes for proposing and approving revisions, along with expected review cycles.

The coalition of industry organizations has agreed to cooperate on several activities in 2020:

- Align the criteria of the NATF model with criteria proposed by other members of the coalition of industry organizations
- Release the aligned model in the first calendar quarter to allow entities to use it while completing process development before the effective date of the NERC supply chain standards
- Develop a web page to disseminate information about the model and on-going development
- Promote awareness of the model and complementary products through in-person and web presentations to key stakeholder groups, registered entities, and the Electric Reliability Organization (ERO) Enterprise
- Test the model in at least one of the available supplier information databases
- Provide additional guidance to entities that:
    - provides ways to use assurance information, along with other factors, in a risk assessment and purchasing decision
    - promotes understanding of the level of assurance and applicability provided by third-party assessments (how to verify that the assessment applies to the product or service to be purchased)
    - describes the types of evidence available for each criterion and the level of assurance for criteria not covered by an industry standard or audit framework
    - provides ways for small entities to apply the model when independent, third-party assessments cannot be utilized

## For More Information

Webpage URL: http://www.natf.net/industry-initiatives/supply-chain-industry-coordination

NATF Contact: supplychain@natf.net

Key Contacts for Industry Organizations: See full listing at: https://www.natf.net/industry-initiatives/supply-chain-industry-coordination/industry-contacts